

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TEXAS  
AUSTIN DIVISION**

CAE INTEGRATED, LLC; CAPITAL  
ASSET EXCHANGE AND TRADING,  
LLC,

Plaintiffs,

v.

MOOV TECHNOLOGIES INC.;  
NICHOLAS MEISSNER,

Defendants.

Case No. 1:21-cv-377

---

**COMPLAINT**

**NATURE OF THE ACTION**

1. This case involves the brazen theft of valuable trade secrets that Plaintiffs CAE Integrated, LLC and Capital Asset Exchange and Trading, LLC (collectively “CAE”) developed over the course of four decades. Defendant Nicholas Meissner (“Meissner”), while an employee of CAE, secretly uploaded thousands of confidential CAE documents onto a personal cloud-based folder. He then left CAE and joined a direct competitor, Defendant Moov Technologies Inc. (“Moov”). Based on evidence CAE has been able to obtain to date, Meissner shared CAE’s trade secrets with Moov, and Moov is leveraging them to rapidly expand its business, giving Moov an unearned competitive advantage against CAE and other market participants. CAE has filed this suit to obtain injunctive, monetary, and other appropriate relief against Meissner and Moov for their theft and unlawful exploitation of its immensely valuable and hard-earned intellectual property.

## **PARTIES**

2. Plaintiff CAE Integrated, LLC is a limited liability company organized and existing under the laws of Texas. Its members have Texas and Colorado citizenship.

3. Plaintiff Capital Asset Exchange and Trading, LLC, is a limited liability company organized and existing under the laws of California. Its members have Texas and Colorado citizenship.

4. Defendant Moov Technologies Inc. is a Delaware corporation with its principal place of business in San Francisco, California.

5. Defendant Nicholas Meissner is a resident of Arizona.

## **JURISDICTION AND VENUE**

6. This Court has subject-matter jurisdiction over the claim arising under the Defend Trade Secrets Act, 18 U.S.C. §§ 1836 *et seq.*, under 28 U.S.C. § 1331. This Court has subject-matter jurisdiction over the state-law claims under 28 U.S.C. § 1367(a). This Court also has subject-matter jurisdiction over the state-law claims under 28 U.S.C. § 1332(a)(1) because there is complete diversity between the parties and the amount-in-controversy exceeds \$75,000.

7. This Court has personal jurisdiction over Defendant Moov because Moov has significant contacts with Texas and this matter arises out of, or relates to, Moov's contacts with Texas and activities that Moov has conducted in Texas. Moov is a registered corporation in the State of Texas, has a mailing address in Austin, Texas, and maintains a registered agent in Austin, Texas. Moov has solicited, and continues to solicit, CAE's Texas-based employees to leave CAE and join Moov. By purposefully targeting and employing ex-CAE employees, Moov has deployed, and is deploying, a strategy of misappropriating the confidential data and trade secrets of a Texas-based company, CAE, causing harm to CAE in Texas. On information and belief, Moov has used CAE's

proprietary data to pitch and secure private investments from one or more Texas citizens and to do business with Texas companies in the semiconductor industry.

8. This Court has personal jurisdiction over Meissner because this matter arises out of, or relates to, the “Employee Nondisclosure, Assignment, Non-Competition And Non-Solicitation Agreement” (hereinafter, “2014 NDA”) that Meissner and CAE Integrated, LLC entered into on or about June 2, 2014, and the 2014 NDA provides that Meissner “irrevocably consent[s] to the exclusive personal jurisdiction of the federal and state courts located in Austin, Texas, as applicable, for any matter arising out of or relating to [the 2014 NDA].” Attachment B, p.7.

9. Additionally, this Court has personal jurisdiction over Meissner because this matter relates to the “Confidential Separation Agreement” (hereinafter, “2018 Confidential Separation Agreement”) that CAE Integrated, LLC and Meissner entered into on July 26, 2018, and that agreement provides that “[f]or any dispute in which an action in court is permitted, [Meissner] submits to, on an exclusive basis, the personal jurisdiction and venue of the state and federal courts located in Austin, Texas, and irrevocably waives any claim that such courts are an inconvenient forum.” Attachment C, p.5.

10. Additionally, this Court has personal jurisdiction over Meissner because he was employed by CAE Integrated, LLC in Austin, Texas, during at least part of the period covered by this complaint, and he committed at least some of the acts alleged in this complaint while residing in Austin, Texas.

11. Venue is proper in this district because a substantial part of the events giving rise to the claims occurred in Austin, Texas. In addition, Defendant Meissner consented to venue in this district in the above-quoted agreements.

## **FACTUAL BACKGROUND**

### **The Opaque Market in Semiconductor Equipment and Commodities**

12. This case concerns the market in used semiconductor equipment. A semiconductor is a substance, most commonly silicon, that conducts electric current, but not with the same degree of conductivity as a full conductor. Semiconductors are used to create integrated circuits, such as microprocessors, which are essential to modern computers and other electronics.

13. Integrated circuits and other semiconductor devices are manufactured in fabrication plants to minutely detailed specifications. Over the course of weeks in a sterile environment, electronic circuits are created on a silicon wafer. This requires the use of a variety of extraordinarily specialized equipment tailored to the needs of a particular fabrication plant: devices such as etchers, evaporators, ion implanters, photoresists, wafer steppers, wafer scrubbers, and wet stations, to name just a few.

14. Many companies operating fabrication plants have their own proprietary methods for creating integrated circuits and other semiconductor devices—technical and chemical processes that they have developed to compete effectively in the market for those products. These companies have a critical interest in keeping their processes and future strategies confidential so that competitors do not learn their methods or plans.

15. Companies that operate fabrication plants regularly decide to purchase or sell used semiconductor equipment. In some instances, a particular device has stopped functioning properly and the plant needs a replacement. In other cases, a plant may be transitioning to a new manufacturing process and therefore may need to purchase new equipment and sell equipment that it no longer needs.

16. For a variety of reasons, absent an appropriate intermediary, the market in used semiconductor equipment would pose extraordinary challenges to any entity that would like to buy

or sell such equipment. Significantly, market participants strongly prefer to conceal their identities from other market participants—who are often their competitors in the integrated-circuit fabrication industry. Competitors in that industry can readily infer from a prospective purchaser's needs, or a prospective seller's offerings, information about the party's proprietary processes for manufacturing integrated circuits or their future direction. For example, a company's offer to sell a particular piece of equipment might indicate to a rival that the seller is transitioning to a new fabrication process. For that reason, market participants generally prefer that transactions occur anonymously.

17. Relatedly, the identities of market participants are not generally known and are not available publicly. Many prospective purchasers, for example, are small fabrication companies or equipment refurbishers in foreign countries that do not have websites and cannot be readily located online. Their contact information may be nothing more than a commercial email address or a local telephone number. That information is not retrievable through ordinary directories or search engines. Even with respect to larger companies with a public footprint, it is often not easily ascertainable which person at the company is responsible for procuring or disposing of a particular type of equipment. Thus, the market for used semiconductor equipment is opaque, and developing the information and connections necessary to create a workable market for these products requires a long and painstaking effort measured in years, if not decades.

18. In addition, semiconductor-device fabrication equipment is so specialized and varied that at any given time there may be only a handful of sellers in the world offering a piece of equipment that satisfies a purchaser's needs. Each of those sellers might be a small mom-and-pop operation somewhere in China or South Korea, with no public presence and no English speakers

on payroll. Working on its own, a prospective purchaser might find it impracticable to locate sellers with regularity for the equipment that it needs.

19. The market has yet another feature that makes it difficult to conduct transactions: the challenge of placing a value on the equipment for sale. There is no government-regulated centralized pricing mechanism, such as a commodities market, for semiconductor-device fabrication equipment. Indeed, typically no public information is released about particular transactions because of the parties' desire for secrecy and anonymity. And most market participants do not conduct transactions with sufficient frequency that they could be confident in their own internal pricing metrics. As a result, absent a private-sector pricing mechanism, parties negotiating a deal would lack the sort of basic pricing and valuation information that parties in other markets take for granted. In other words, historical transaction and pricing information—like the identity of the market players themselves—is largely invisible to the public and very valuable in creating and operating a market for these transactions.

### **CAE's Industry-Leading Innovations**

20. CAE solves these critical problems in the market for used semiconductor equipment by matching buyers and sellers through its proprietary platform. CAE traders use CAE's highly sophisticated platform, which has been painstakingly constructed from data accumulated over decades, to identify and contact parties to transactions in used semiconductor equipment and to provide the parties accurate price ranges and other information about the equipment for sale. CAE takes title to equipment from sellers and then resells it to purchasers, ensuring anonymity for the parties.<sup>1</sup>

---

<sup>1</sup> Plaintiffs CAE Integrated, LLC and Capital Asset Exchange & Trading, LLC are limited liability companies with the same members. Each is responsible for particular aspects of CAE's business. Capital Asset Exchange & Trading, LLC is the entity that enters into contracts with customers. Each of the two entities employs traders and other

21. CAE was founded in 1982 as the market for semiconductor equipment was first emerging. In the era before wide access to the Internet, CAE started by offering a print catalog.

22. As it gradually expanded through the 1980s and 1990s, CAE accumulated a wealth of knowledge about which sellers around the world offered the thousands of types of semiconductor equipment; the particular requirements of prospective purchasers; the valuation of each type of equipment; and other information integral to the transactions that it enabled.

23. In the 1990s, CAE first started organizing this web of information about purchasers, sellers, and equipment into a centralized database. The first iterations of its database were constructed using commercially available software.

24. CAE went online in the 1990s, reaching a broader set of purchasers and sellers. It started actively putting together deals in semiconductor equipment, earning revenue by charging commissions on the sales that it facilitated.

25. In the late 2000s, CAE underwent another evolution to its current form. It switched its business model from a commission-based approach to an arbitrage model. Rather than introducing buyers and sellers and charging a commission, CAE now takes title to an asset from the seller and then resells it to the purchaser. To ensure anonymity, the transaction occurs in a black box; neither purchaser nor seller knows the identity of the other. CAE retains the spread between what the purchaser pays and what the seller receives.

26. By the late 2000s, CAE's database contained decades' worth of data that had been steadily accumulated since the founding of the company. But the commercially available database software proved inadequate to the increasing complexity and sophistication of CAE's business. So in 2013, CAE hired a third-party software company to build a proprietary platform tailored to

---

employees. Employees at both entities acquire, create, and use the trade-secret information described in this complaint, and the operations of the two entities are fully integrated.

the semiconductor-equipment industry and CAE's unique needs. CAE later created an in-house software-engineering team to continually improve its platform. That team now has over twenty members.

27. CAE's proprietary platform collects, categorizes, and analyzes a massive amount of data from business transactions in a way that allows CAE to anticipate the needs of purchasers and sellers across the world and to surpass its competitors in detailed knowledge of the thousands of pieces of equipment that market participants seek to buy and sell. At this point the platform encompasses nearly 40 years of data on transactions in semiconductor equipment that CAE facilitated, giving CAE deep and unique insights into the global market for those products. That data was slowly and painstakingly acquired over those four decades through tens of thousands of individual transactions and interactions with customers.

28. The database was built, and continues to expand, through the daily work of individual traders. Each time a CAE trader conducts a transaction or discusses a potential transaction with a market participant, information about the transaction is entered into the database by a team of data-entry specialists or by automated proprietary software that CAE's in-house software team has created. This ensures that CAE mines and records virtually all relevant data generated by its traders during their interactions with clients. Through that slow, structured process of accretion, CAE has developed a proprietary database that gives CAE a hard-earned competitive advantage in its industry.

29. The database provides traders with real-time information to help complete transactions. For example, when a relevant asset or requirement is generated through another trader's client interaction in our market, the platform immediately circulates a notification to all traders



working with sellers that might be offering that equipment. Traders can also conduct searches within the database to locate prospective purchasers or sellers.

30. In addition, the database provides traders with detailed information about products—not only information about pricing, makes, models, and product configurations, but also information that traders without technical backgrounds can use to ask a prospective customer the appropriate questions regarding a contemplated transaction. That information exists only because CAE spent years accumulating data on tens of thousands of products.

31. CAE estimates it has spent over 100,000 worker-hours—valued at millions of dollars—prototyping, developing, coding, testing, deploying, and modifying its proprietary technology.

32. As part of their training, traders are taught particular methods to elicit important data from transacting parties. For example, traders are advised to ask specific questions to learn additional information about a company or a piece of equipment. Through that standardized process, CAE acquires more data, which in turn makes its platform more precise and comprehensive, and better able to predict the behavior of market participants.

33. As a result of its hard work and incredible innovations in data acquisition and analysis, CAE expanded rapidly in the late 2000s and 2010s. From a handful of employees in the 1980s and 1990s, CAE now employs almost 200 people in the United States and around the world. Many employees work full-time managing, expanding, and improving its proprietary platform. It is the leading company worldwide in market-making for sales of used semiconductor equipment.

#### **CAE's Valuable Trade Secrets**

34. CAE holds two distinct categories of trade secrets relevant here: (i) the data about its clients and the equipment it buys and sells that its traders collect and enter into the database at

the heart of CAE's proprietary platform; and (ii) the proprietary platform itself, which was custom-designed to the semiconductor-equipment industry and CAE's innovative, data-driven business model.

35. *Customer and transaction data.* CAE's traders collect and record a variety of data about customers, equipment, and specific transactions. Those include:

- a. CAE's lists of past, current, and prospective customers.
- b. CAE's customer listings and requirements.
- c. CAE's list of actual and prospective sellers and the following seller-related

information:

- i. Equipment previously sold, identities of buyer and seller, date of sale, original asking price, actual sale price, condition and configuration of equipment at time of sale, and the reason the equipment was being sold;
- ii. Equipment currently for sale, asking price, condition and configuration of equipment for sale, and the reason the equipment is for sale;
- iii. Equipment that may be available for sale, timing of a potential sale, potential asking price, condition and configuration of equipment, and the reason the equipment may be for sale;
- iv. Equipment installed and equipment being used;
- v. Equipment seller does *not* use or deal in;
- vi. Historical sales activity, historical change in prices, projected future sales activity, and details of deal discussions;
- vii. Identification of, and contact information for, specific seller contacts within selling entity and their roles and responsibilities; and

viii. Relationships between brokers, agents, and sellers and the listing of what information brokers and agents have concerning specific sellers.

d. CAE's list of actual and prospective buyers and the following buyer-related information:

i. Equipment previously purchased, identities of buyer and seller, date of purchase, original asking price, actual sale price, condition and configuration of equipment at time of sale, and the reason the equipment is being purchased;

ii. Equipment being searched for, range of potential purchase price, condition and configuration of equipment needed, and timing of purchase;

iii. Equipment that may be sought for purchase, timing of potential purchase, potential buying price, condition and configuration of equipment sought, and the reason the equipment may be purchased;

iv. Equipment currently installed and equipment being used;

v. Historical purchasing activity, historical change in prices paid, projected future purchase activity, and detail of deal discussions;

vi. Identification of, and contact information for, specific buyer contacts within purchasing entity and their roles and responsibilities;

vii. Relationships between brokers, agents, and buyers and the listing of what information brokers and agents have concerning specific buyers; and

viii. Identification of buyers' expertise, market role, and re-sale history.

e. CAE's asset marketing strategy for specific equipment.

f. CAE's trader training materials and instructions.

36. *CAE's proprietary platform.* CAE's platform was custom-designed to aggregate and analyze the massive amount of data that the company has acquired over four decades and to be uniquely effective at enabling traders to complete deals in the semiconductor-equipment industry. CAE has a full-time staff that continually improves the platform.

### **CAE's Efforts to Safeguard Its Trade Secrets**

37. Given the immense value of its data about customers and equipment, CAE has taken extensive measures to keep the data secure and confidential.

38. *Limited, Monitored Access for Employees.* CAE uses software that prevents employees from accessing the company's data unless they are within CAE's offices or are remotely accessing the network with a CAE-issued device through a virtual private network requiring two-factor authentication. CAE also employs software to monitor all employee access to confidential data. That software tracks employee activity on their devices, including through the use of screenshots, and it sends reports to CAE management.

39. CAE restricts the third-party applications that employees may download to their devices that could interact with or capture the company's data.

40. CAE has implemented a variety of physical security measures, including badge access to its offices, and CAE highly restricts access to its servers.

41. *Security Against Outside Threats.* CAE employs top-of-the-line network security software to protect against outside threats to its data, such as hacking efforts emanating from China and Russia.

42. *Employee Agreements.* CAE requires employees to sign a non-disclosure agreement, which includes non-disclosure provisions, among other provisions (such as non-compete and non-solicitation provisions). *See* para. 45, 47, *infra*. The non-disclosure agreement specifies

that a wide variety of CAE's confidential information, including customer information, may not be disclosed to outside parties. CAE reminds departing employees of their obligations under these agreements.

43. *Training and Reminders.* CAE provides extensive training to new employees on data confidentiality and security. In addition, CAE management sends regular reminders to employees about their legal obligations and the importance of maintaining the confidentiality of data.

### **Meissner's Theft of CAE's Trade Secrets**

44. Meissner was hired by Capital Asset Exchange and Trading, LLC as a trader in 2008 in California. As with other traders, his position required him to use CAE's confidential and proprietary database to match buyers and sellers of semiconductor equipment. Meissner had privileged and restricted access to CAE's entire database of proprietary information throughout his decade of employment with CAE.

45. On or about April 12, 2012, Meissner entered into an agreement with Capital Asset Exchange and Trading, LLC, entitled "Confidential Information and Invention Assignment Agreement" (hereinafter, "2012 Confidential Information Agreement"). Attachment A. In exchange for his continued employment, he made a series of promises to Capital Asset Exchange and Trading, LLC.

a. Meissner "agree[d] at all times during the [employment relationship] and thereafter, to hold in strictest confidence, and not to use, except for the benefit of Company to the extent necessary to perform my obligations to the Company under the [employment relationship], or to disclose to any person, firm, corporation or other entity without written authorization of the Board of Directors of the Company, any Confidential Information of the Company which I obtain or create." He "further agree[d] not to make copies of such

Confidential Information except as authorized by the Company.” The term “Confidential Information” was defined to include “any Company proprietary information, technical data, trade secrets, or know-how, including, but not limited to, research, product plans, products, services, suppliers, customer lists and customers (including, but not limited to, customers of the Company on whom I called or with whom I became acquainted during the [employment relationship], prices and costs, markets, software, . . . budgets or other business information disclosed to me by the Company . . . or created by me during the [employment relationship].” Attachment A, pp.1–2.

b. Meissner also “recognize[d] that the Company has received and in the future will receive confidential or proprietary information from third parties subject to a duty on the Company’s part to maintain the confidentiality of such information” and “agree[d] to hold all such confidential and proprietary information in the strictest confidence and not to disclose it to any person, firm or corporation or to use it except as necessary in carrying out my work for the Company consistent with the Company’s agreement with such third party.” Attachment A, p. 2.

c. Meissner “agree[d] that, at the time of termination of the [employment relationship], I will deliver to the Company (and will not keep in my possession, recreate, or deliver to anyone else) any and all devices, records, data, notes, reports, proposals, lists, correspondence, specifications, . . . other documents or property, or reproductions of any of the aforementioned items developed by me pursuant to the [employment relationship] or otherwise belonging to the Company.” Attachment A, p.4.

d. Meissner agreed that “during the [employment relationship] and at any time following termination of the [employment relationship] for any reason, with or without

cause, I shall not use any Confidential Information of the Company to attempt to negatively influence any of the Company's clients or customers from purchasing Company products or services or to solicit or influence or attempt to influence any client, customer or other person either directly or indirectly, to direct his or its purchase of products and/or services to any person, firm, corporation, institution or other entity in competition with the business of the Company." Attachment A, p.5.

46. In 2014, Meissner became an employee of CAE Integrated, LLC and moved from California to Austin, Texas.

47. On or about June 2, 2014, Meissner signed the 2014 NDA with CAE Integrated, LLC. Under the 2014 NDA, which was substantially the same as the non-disclosure agreements that other CAE employees signed, Meissner agreed that, in exchange for his employment, he "will not disclose any Proprietary Information to anyone outside [the] Company." Attachment B, p.3.

The agreement defined "Proprietary Information" to include:

(a) any information that is confidential or proprietary, . . . including for example and without limitation, information related to Company Innovations . . . , concepts, techniques, processes, methods, systems, designs, computer programs, source documentation, trade secrets, formulas, development or experimental work, work in progress, forecasts, proposed and future products, marketing plans, business plans, customers and suppliers and any other nonpublic information that has commercial value or (b) any information Company has received from others that Company is obligated to treat as confidential or proprietary . . . .

Attachment B, p.3.

48. In signing the 2014 NDA, Meissner further agreed that "[a]t any time upon Company's request, and when my employment with Company is over, I will return all materials . . . containing or disclosing any Proprietary Information (including all copies thereof)." Attachment B, p.5.

49. In 2015, Meissner became a member of CAE Integrated, LLC, with a small equity interest. That equity interest was later converted into an equity interest in Capital Asset Exchange & Trading, LLC.

50. During his employment at CAE, Meissner was issued various computers and phones to use for work-related matters.

51. In approximately 2012, CAE issued Meissner an Apple Macintosh laptop. In 2016, CAE issued Meissner a different laptop that was better able to integrate with CAE's information-technology and security infrastructure, including the monitoring software that CAE employed to track what employees were doing with their company-issued devices. CAE then requested that Meissner return the Macintosh. Meissner initially refused, maintaining that he had no obligation to return the computer, despite the fact that CAE had provided it to him. He ultimately relented and returned the laptop to CAE.

52. In January 2021, after CAE received indications that Meissner was sharing confidential trade secrets with his new employer, Defendant Moov, CAE commissioned a forensic analysis of the laptop. The results were stunning.

53. Between 2013 and 2016, Meissner uploaded *thousands* of confidential CAE documents to a Google Drive folder linked to his personal Gmail address.

54. Meissner had no legitimate purpose related to his responsibilities at CAE for uploading CAE documents to a Google Drive folder linked to his personal email address. Employees, including Meissner, were frequently reminded that CAE policy prohibited the use of a personal cloud folder to store confidential CAE documents absent management approval, which



Meissner did not obtain. Indeed, his actions immediately put the confidentiality of those documents at risk because CAE's information-security measures did not cover Meissner's personal Google Drive folder.

55. Meissner's means for uploading the documents was brazen—and revealed why he was so reluctant to return the Macintosh laptop to CAE. Meissner, using the Google Drive app, created a "synchronization folder" on the Macintosh. As the name indicates, that folder would synchronize with a Google Drive folder stored on the cloud. Meissner would then drag confidential materials—such as PDFs of purchase agreements and invoices with CAE customers—into the synchronization folder. As a result, a copy of each of those files was automatically saved in the cloud folder linked to his personal email address.

56. The thousands of CAE files contained in the synchronization folder on the Macintosh (and therefore uploaded to Meissner's personal cloud drive) encompassed numerous CAE confidential materials. They included:

- a. Hundreds of documents memorializing or otherwise relating to completed deals (some of which Meissner had no role in executing, further confirming that he had no conceivable business purpose for saving the documents outside of CAE's infrastructure). Each of those documents contains up to twenty data elements that CAE traders regularly enter into the company's proprietary platform—for example, the identities of the purchasers and sellers, the purchaser's needs, the seller's assets, the points of contact at each party, the particular specification of the equipment sold, and the price that the parties agreed to.
- b. Numerous proprietary models that CAE has developed to guide traders who lack a technical background in understanding and valuing semiconductor equipment.

c. Folders for the most commonly traded equipment, which included configurations, diagrams, and “cheat sheets” containing information about equipment.

57. Taken together, this information comprised much of what a CAE competitor would need to create a rival platform. A start-up competitor faces a fundamental challenge in building a platform that can compete with an established market participant like CAE: Without a critical mass of data about potential buyers and sellers of semiconductor equipment and past transactions, it is difficult to seed a new platform with enough data to provide useful insights into market participants, equipment, and pricing. But most of the necessary information is not publicly available, and it would take painstaking efforts over a long period of time to compile the information through interactions with market participants.

58. As a consequence, it would take many years for a rival to construct (through honest means) a platform to compete with CAE’s platform, which was 40 years in the making. But what Meissner uploaded to his personal cloud drive, which encompasses an estimated ten to fifteen years’ worth of accumulated information collected and organized by CAE, would give a rival the building blocks to construct its own platform immediately.

59. Based on the forensic analysis, Meissner carried out this misappropriation of CAE’s confidential documents and trade secrets from at least 2013 to 2016.

60. Meissner left CAE in 2018.

61. On or about July 26, 2018, Meissner entered into the 2018 Confidential Separation Agreement with CAE Integrated, LLC in which CAE bought back his equity stake and agreed to release certain claims against him in exchange for various promises. Attachment C.

a. Meissner “agree[d] that he shall continue to be bound and abide by the [2014 NDA].” Attachment C, p.3,

b. He further represented and agreed that he had returned to CAE Integrated, LLC “all Company property in his possession, including, but not limited to, originals and all copies of Company files, work product, electronic mail, . . . confidential and/or trade secret information, [and] company documents,” as well as “any files or documents related to the Company or any of the Company Entities, including any pertaining to or reflecting Proprietary Information (as defined in the 2014 NDA), that [he] may maintain or have stored at his residence, on his personal electronic devices, on his personal email or cloud storage accounts, or elsewhere.” Attachment C, p.3.

c. Meissner also “agree[d] that he will not disparage or make negative statements or unfavorable comments (or induce or encourage others to disparage or make negative statements or unfavorable comments) about the Company entities[.]” Attachment C, p.4.

### **Meissner Joins Direct CAE Competitor Moov And Defendants Use CAE’s Data to Compete with CAE**

62. Approximately one year after he ended his employment at CAE (soon after the expiration of his non-compete period), Meissner was hired by Defendant Moov as its Head of Sales.

63. Moov was founded in 2017 in San Francisco by two other former employees of CAE, Steven Zhou and Maxam Yeung. Moov touts itself as “the world’s first real-time interactive platform for buying and selling used manufacturing equipment.”<sup>2</sup> The company appears to focus almost exclusively on used semiconductor equipment and closely related technology.<sup>3</sup> Moov is a direct competitor of CAE.

---

<sup>2</sup> [www.moov.co](http://www.moov.co) (last accessed Apr. 29, 2021).

<sup>3</sup> See [www.moov.co/browse](http://www.moov.co/browse) (last accessed Apr. 29, 2021).

64. Moov claims to have over ten thousand active listings and to list over \$1 billion of equipment value.<sup>4</sup>

65. According to a Moov press release:

Moov is at the center of a hidden economy inside high-tech manufacturing. . . .

Moov's real-time, self-serve marketplace matches buyers and sellers around the world, eliminating waste by placing used products back into the value chain. Moov's software automates documentation, information sharing, and the entire transaction process, including contracts, payments, logistics and add-on services, allowing companies to buy and sell with ease.<sup>5</sup>

66. Moov boasts to employees within the company and, on information and belief, has claimed to potential investors and customers, that it has built a platform for buying and selling semiconductor equipment that is superior to CAE's platform.

67. For the reasons explained above, building a database of the size and efficiency that Moov claims it has built—through honest means—would take decades of painstaking acquisition and analysis of data from thousands of transactions. It is not plausible that in the four years since its founding in 2017 Moov has legitimately acquired a sufficient quantity of data in the exceedingly opaque market for used semiconductor equipment to create the sort of massive database that it touts to its employees and prospective customers and investors.

68. Moov's business strategy has included targeting current and former CAE employees to leave CAE and join Moov. Moov has in fact hired multiple former CAE employees, including Meissner, to fill key roles. All of those ex-employees are bound by an NDA that prohibits them from disclosing CAE's trade secrets and other confidential information. Notwithstanding,

---

<sup>4</sup> [www.moov.co](http://www.moov.co) (last accessed Apr. 29, 2021).

<sup>5</sup> <https://www.businesswire.com/news/home/20200122005227/en/Moov-Closes-2.4M-in-Seed-Funding-to-Accelerate-Growth-of-the-World%E2%80%99s-First-Real-Time-Used-Manufacturing-Equipment-Marketplace> (last accessed Apr. 29, 2021).

on information and belief, Moov's strategy is to bring on former CAE employees and obtain from them CAE's confidential information, which it then uses to build its own platform.

69. Based on information gathered to date, Meissner shared with Moov CAE's confidential data and trade secrets that he uploaded to his personal Google Drive—including documents containing critical information about customers, equipment, and transactions—to enable Moov to build its rival platform and to confer on Moov an unearned competitive advantage against CAE and other market participants.

70. Based on information gathered to date, Moov has conducted or attempted to conduct transactions with CAE customers who could not readily be located through public sources by exploiting CAE's confidential information misappropriated by Meissner.

71. On information and belief, Moov has built a database that replicates key features of CAE's proprietary database, including automated notifications, assets models, and customer behavioral models.

72. Following Meissner's hiring at Moov as Head of Sales, Moov issued multiple press releases announcing that the company has received millions of dollars in new investment capital from a variety of investors. On information and belief, Moov touted its data platform in soliciting these investments and described its database to investors as the product of its own innovations, but it was based on data and concepts misappropriated from CAE. On information and belief, Moov has made the same claims to customers.

**COUNT ONE (All Defendants)**  
**Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq.***

73. Paragraphs 1-72 are realleged as if fully set forth herein.

74. In connection with their transactions in semiconductor equipment and related products, Plaintiffs and Defendants are engaged in interstate and international commerce.

75. CAE's confidential and proprietary information includes (but is not limited to) the information set forth in paragraph 34-36, including customer lists; customer contact information; information about customers' requirements, preferences, and inventory; information about valuation and pricing of equipment; and records of transactions conducted by or facilitated by CAE. In addition, CAE's platform for aggregating, organizing, and analyzing this information is proprietary and confidential.

76. Each category of CAE's proprietary and confidential information is a trade secret within the meaning of 18 U.S.C. § 1839(3).

77. CAE derives economic value and competitive advantage from this information not being known or used by its competitors or others.

78. CAE has taken appropriate steps to ensure the confidentiality of this information, including state-of-the-art information-security measures, such as password protection and limitations on the use of non-approved applications and programs to access the information; physical restrictions on access to CAE's offices; technological restrictions on how employees may access this information; and non-disclosure agreements with its employees and others, including with Defendant Meissner.

79. Defendants have each misappropriated CAE's trade secrets in violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq.*

80. In violation of CAE's well-established policies, Defendant Meissner, while still employed at CAE, uploaded a substantial quantity of CAE's trade secrets to a personal cloud drive.

81. In breach of multiple confidentiality agreements that he signed, Meissner shared the trade secrets that he misappropriated with Defendant Moov in order to give Moov an unearned competitive advantage against CAE and other market participants.

82. Moov knew or should have known that the trade secrets had been acquired and disclosed by Meissner by improper means, *i.e.*, through theft, misrepresentation, and/or a violation of a duty to maintain the secrecy of the trade secrets.

83. CAE did not authorize Meissner to disclose the trade secrets to Moov and did not authorize Moov to acquire or use the trade secrets.

84. Defendants are using, or intend to use, CAE's misappropriated trade secrets to gain a competitive advantage against CAE and other market participants.

85. CAE has sustained, and will continue to sustain, damages as the result of Defendants' misappropriation and use of its trade secrets.

86. CAE has sustained, and will continue to sustain, irreparable harm as a result of Defendants' misappropriation and use of its trade secrets.

87. Defendants have been unjustly enriched by their misappropriation and use of CAE's trade secrets.

88. Because Defendants' misappropriation was willful and malicious, CAE is entitled to exemplary damages under 18 U.S.C. § 1836(b)(3)(C).

**COUNT TWO (All Defendants)**  
**Texas Uniform Trade Secrets Act,**  
**Tex. Civ. Prac. & Rem. Code §§ 134A *et seq.***

89. Paragraphs 1-88 are realleged as if fully set forth herein.

90. In connection with their transactions in semiconductor equipment and related products, both CAE and Moov are engaged in commerce in the State of Texas as well as in other States and foreign nations.

91. CAE's confidential and proprietary information includes (but is not limited to) the following: customer lists; customer contact information; information about customers' requirements, preferences, and inventory; information about valuation and pricing of equipment; and records of transactions conducted by or facilitated by CAE. In addition, CAE's platform for aggregating, organizing, and analyzing this information is proprietary and confidential.

92. Each category of CAE's proprietary and confidential information is a trade secret within the meaning of Tex. Civ. Prac. & Rem. Code § 134A.002(6).

93. CAE derives economic value and competitive advantage from this information not being known or used by its competitors or others.

94. CAE has taken appropriate steps to ensure the confidentiality of this information, including state-of-the art information-security measures, such as password protection and limitations on the use of non-approved applications and programs to access the information; physical restrictions on access to CAE's offices; technological restrictions on how employees may access this information; and non-disclosure agreements with its employees and others, including with Defendant Meissner.

95. Defendants have each misappropriated CAE's trade secrets in violation of the Texas Uniform Trade Secrets Act, Tex. Civ. Prac. & Rem. Code §§ 134A *et seq.*

96. In violation of CAE's well-established policies, Defendant Meissner, while still employed at CAE, uploaded a substantial quantity of CAE's trade secrets to a personal cloud drive.

97. In breach of multiple confidentiality agreements that he signed, Meissner shared the trade secrets that he misappropriated with Defendant Moov in order to give Moov an unearned competitive advantage against CAE and other market participants.



98. Moov knew or should have known that the trade secrets had been acquired and disclosed by Meissner by improper means, *i.e.*, through theft, misrepresentation, and/or a violation of a duty to maintain the secrecy of the trade secrets.

99. CAE did not authorize Meissner to disclose the trade secrets to Moov and did not authorize Moov to acquire or use the trade secrets.

100. Defendants are using, or intend to use, CAE's misappropriated trade secrets to gain a competitive advantage against CAE and other market participants.

101. CAE has sustained, and will continue to sustain, damages as the result of the Defendants' misappropriation and use of its trade secrets.

102. CAE has sustained, and will continue to sustain, irreparable harm as a result of the Defendants' misappropriation and use of its trade secrets.

103. Defendants have been unjustly enriched by their misappropriation and use of CAE's trade secrets.

104. Because Defendants' misappropriation was willful and malicious, CAE is entitled to exemplary damages and attorney's fees under Tex. Civ. Prac. & Rem. Code §§ 134A.004(b) and 134A.005(3).

**COUNT THREE (Meissner Only)**  
**Breach of Contract (Texas and California Common Law)**

105. Paragraphs 1-104 are realleged as if fully set forth herein.

106. On or about April 12, 2012, Meissner entered into the 2012 Confidential Information Agreement with Capital Asset Exchange and Trading, LLC. In exchange for his continued employment, Meissner "agree[d] that at all times during the [employment relationship] and thereafter, to hold in strictest confidence, and not to use, except for the benefit of Company to the extent necessary to perform my obligations to the Company under the [employment relationship], or to

disclose to any person, firm, corporation or other entity without written authorization of the Board of Directors of the Company, any Confidential Information of the Company of which I obtain or create.” He “further agree[d] not to make copies of such Confidential Information except as authorized by the Company.” The term “Confidential Information” was defined to include “any Company proprietary information, technical data, trade secrets, or know-how, including, but not limited to, research, product plans, products, services, suppliers, customer lists and customers (including, but not limited to, customers of the Company on whom I called or with whom I became acquainted during the [employment relationship]), prices and costs, markets, software, . . . budgets or other business information disclosed to me by the Company . . . or created by me during the [employment relationship].”

107. Under the 2012 Confidential Information Agreement, Meissner “recognize[d] that the Company has received and in the future will receive confidential or proprietary information from third parties subject to a duty on the Company’s part to maintain the confidentiality of such information” and “agree[d] to hold all such confidential or proprietary information in the strictest confidence and not to disclose it to any person, firm or corporation or to use it except as necessary in carrying out my work for the Company consistent with the Company’s agreement with such third party.”

108. Under the 2012 Confidential Information Agreement, Meissner “agree[d] that, at the time of termination of the [employment relationship], I will deliver to the Company (and will not keep in my possession, recreate, or deliver to anyone else) any and all devices, records, data, notes, reports, proposals, lists, correspondence, specifications, . . . other documents or property, or reproductions of any of the aforementioned items developed by me pursuant to the [employment relationship] or otherwise belonging to the Company[.]”

109. Under the 2012 Confidential Information Agreement, Meissner agreed that “during the [employment relationship] and at any time following termination of the [employment relationship] for any reason, with or without cause, I shall not use any Confidential Information of the Company to attempt to negatively influence any of the Company’s clients or customers from purchasing Company products or services or to solicit or influence or attempt to influence any client, customer or other person either directly or indirectly, to direct his or its purchase of products and/or services to any person, firm, corporation, institution or other entity in competition with the business of the Company.”

110. Under the 2012 Confidential Information Agreement, Meissner “acknowledge[d] and agree[d] that violation of this Agreement by me may cause the Company irreparable harm, and therefore agree[d] that the Company will be entitled to seek extraordinary relief in court, including but not limited to temporary restraining orders, preliminary injunctions and permanent injunctions without the necessity of posting a bond or other security . . . .”

111. The 2012 Confidential Information Agreement provides that it “shall be governed by the laws of the State of California.”

112. On or about June 2, 2014, Meissner entered into the 2014 NDA with CAE Integrated, LLC. In exchange for his employment, Meissner agreed that he “will not disclose any Proprietary Information to anyone outside [the] Company.” The agreement defined “Proprietary Information” in part to include “any information that is confidential or proprietary, . . . including for example and without limitation, information related to Company Innovations . . . , concepts, techniques, processes, methods, systems, designs, computer programs, source documentation, trade secrets, formulas, development or experimental work, work in progress, forecasts, proposed

and future products, marketing plans, business plans, customers and suppliers and any other non-public information that has commercial value.” The agreement further defined “Proprietary Information” to include “any information Company has received from others that Company is obligated to treat as confidential or proprietary.”

113. Under the 2014 NDA, Meissner agreed that “[a]t any time upon Company’s request, and when my employment with Company is over, I will return all materials . . . containing or disclosing any Proprietary Information (including all copies thereof)[.]”

114. The 2014 NDA provides that “[t]his Agreement . . . shall survive [Meissner’s] employment by Company . . . .”

115. Under the 2014 NDA, Meissner “agree[d] that if I violate this Agreement, Company will suffer irreparable and continuing damages for which money damages are insufficient, and Company shall be entitled to injunctive relief and/or a decree for specific performance, and such other relief as may be proper (including money damages if appropriate), to the extent permitted by law.”

116. The 2014 NDA provides that it “shall be governed by the laws of the United States of America and by the laws of the State of Texas, as such laws are applied to agreements entered into and to be performed entirely within Texas between Texas residents.”

117. On or about July 26, 2018, Meissner entered into the 2018 Confidential Separation Agreement with CAE Integrated, LLC in which CAE Integrated, LLC bought back his equity stake in Capital Asset Exchange and Trading, LLC, and agreed to release certain claims against him in exchange for various promises. Meissner “agree[d] that he shall continue to be bound and abide by the [2014 NDA] executed by Employee on or about June 2, 2014.” He further represented and agreed that he had returned to CAE “all Company property in his possession, including, but not

limited to, original and all copies of Company files, work product, electronic mail, . . . confidential and/or trade secret information, [and] company documents,” as well as “any files or documents related to the Company or any of the Company Entities, including any pertaining to or reflecting Proprietary Information (as defined in the 2014 NDA), that [he] may maintain or have stored at his residence, on his personal electronic devices, on his personal email or cloud storage accounts, or elsewhere.”

118. Meissner also “agree[d] that he will not disparage or make negative statements or unfavorable comments (or induce or encourage others to disparage or make negative statements or unfavorable comments) about the Company Entities[.]”

119. The 2018 Confidential Separation Agreement provides that the foregoing provisions “shall in all respects be governed and construed in accordance with the laws of the State of Texas, without regard to its conflicts of law provisions.”

120. Capital Asset Exchange and Trading, LLC, has performed all of its obligations under the 2012 Confidential Information Agreement, and CAE Integrated, LLC has performed all of its obligations under the 2014 NDA and the 2018 Confidential Separation Agreement. Any conditions precedent have been satisfied.

121. Meissner breached each of the foregoing contractual provisions relating to confidential information. While still employed at CAE Integrated, LLC, he uploaded a substantial quantity of CAE’s trade secrets to a personal cloud drive. He then shared the trade secrets that he misappropriated with Defendant Moov in order to give Moov an unearned competitive advantage against CAE and other market participants.

122. CAE has sustained, and will continue to sustain, damages as the result of Meissner’s contractual breaches.

123. CAE has sustained, and will continue to sustain, irreparable harm as a result of Meissner's contractual breaches.

**COUNT FOUR (Meissner Only)**  
**Fraud in the Inducement (Texas Common Law)**

124. Paragraphs 1-122 are realleged as if fully set forth herein.

125. At the time that Meissner entered into the 2014 NDA and the 2018 Confidential Separation Agreement, he had no intention to comply with the provisions of those agreements quoted in paragraphs 47-48 and 61 of this Complaint relating to the nondisclosure of confidential information and trade secrets. In fact, at the time he entered into the agreements, he had already secretly uploaded confidential information and trade secrets to a personal cloud account. He therefore made material misrepresentations in the agreements that he knew were false at the time.

126. Meissner's misrepresentations were intended to induce CAE Integrated, LLC to enter into the 2014 NDA and the 2018 Confidential Separation Agreement, in which CAE provided valuable consideration. CAE Integrated, LLC reasonably relied on the misrepresentations in entering into the agreements.

127. CAE has sustained, and will continue to sustain, damages as the result of its reliance on Meissner's fraudulent misrepresentations.

128. CAE has sustained, and will continue to sustain, irreparable harm as a result of Meissner's fraudulent misrepresentations.

**COUNT FIVE (Meissner Only)**  
**Breach of Fiduciary Duty (Texas and California Common Law)**

129. Paragraphs 1-128 are realleged as if fully set forth herein.

130. As an employee and member at various points in time of both CAE Integrated, LLC and Capital Asset Exchange and Trading, LLC, Meissner had a fiduciary relationship with those entities.

131. In violation of CAE's well-established policies, Meissner, while employed at CAE, uploaded a substantial quantity of CAE's trade secrets to a personal cloud drive.

132. In breach of multiple confidentiality agreements that he signed, Meissner shared the trade secrets and confidential information that he misappropriated with Defendant Moov in order to give Moov an unearned competitive advantage against CAE and other market participants.

133. CAE did not authorize Meissner to disclose confidential information to Moov and did not authorize Moov to acquire or use the confidential information.

134. Meissner accordingly breached his fiduciary duties to CAE, including the duty of loyalty and the duty of obedience.

135. CAE has sustained, and will continue to sustain, damages as the result of Meissner's breach of his fiduciary duties.

136. CAE has sustained, and will continue to sustain, irreparable harm as a result of Meissner's breach of his fiduciary duties.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs respectfully request entry of judgment in their favor and against Defendants. Plaintiffs seek the following measures of relief:

A. A preliminary and permanent injunction:

1. Prohibiting Meissner from using, disclosing, disseminating, distributing, or discussing CAE's trade secrets or confidential information;

2. Directing Meissner to destroy all copies of CAE's trade secrets or confidential information that are in his possession, custody, or control and any information derived, directly or indirectly, from CAE's trade secrets or confidential information that is in his possession, custody, or control;

3. Prohibiting Moov from using, disclosing, disseminating, distributing, or discussing CAE's trade secrets or confidential information;

4. Directing Moov to destroy all copies of CAE's trade secrets or confidential information in its possession, custody, or control and any information derived, directly or indirectly, from CAE's trade secrets or confidential information that is in its possession, custody, or control, including by purging such information from its databases, records, files, computers, and other media and data storage sources.

5. Prohibiting any of Moov's officers, agents, servants, employees, and attorneys, or any persons or entities who are in active concert or participation with Meissner, Moov, or any of Moov's officers, agents, servants, employees, and attorneys, from using, disclosing, disseminating, distributing, or discussing CAE's trade secrets or confidential information; and

6. Directing any of Moov's officers agents, servants, employees, and attorneys, or any persons or entities who are in active concert or participation with Meissner, Moov, or any of Moov's officers, agents, servants, employees, and attorneys, from using, disclosing, disseminating, distributing, or discussing CAE's trade secrets or confidential information.



B. Statutory, compensatory, exemplary, and punitive damages, in an amount to be proven at trial, caused by Defendants' violations of the Defend Trade Secrets Act, the Texas Uniform Trade Secrets Act, and Texas and California common law;

C. Attorneys' fees and costs associated with prosecuting this action;

D. Prejudgment and post-judgment interest;

E. A declaration that Defendants are liable for all past and future costs and damages caused by the actions alleged herein; and

F. Such other or additional relief as this Court deems just and proper under the circumstances.

DATED: April 29, 2021

Respectfully submitted,

QUINN EMANUEL URQUHART &  
SULLIVAN, LLP

/s/ John Bash

John Bash  
Texas Bar No. 24067504  
johnbash@quinnemanuel.com  
Scott Cole  
Texas Bar No. 00790481  
scottcole@quinnemanuel.com  
201 West 5th Street, 11th Floor  
Austin, Texas 78701  
737.667.6100 – Telephone  
737.667.6110 – Facsimile

John Robinson (*Pro Hac Vice Forthcoming*)  
johnrobinson@quinnemanuel.com  
191 N. Wacker Drive, Suite 2700  
Chicago, Illinois 60606  
312.705.7400 – Telephone  
312.705.7401 – Facsimile

*Attorneys for Plaintiffs CAE Integrated, LLC and  
Capital Asset Exchange and Trading, LLC*